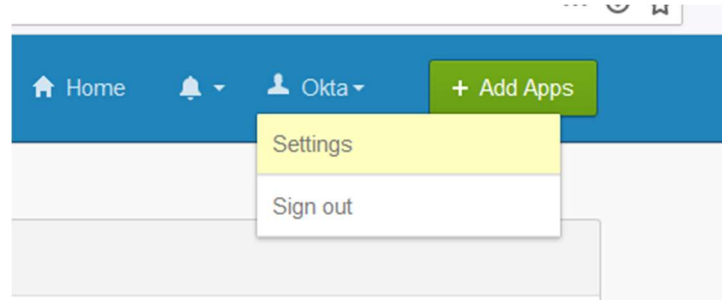


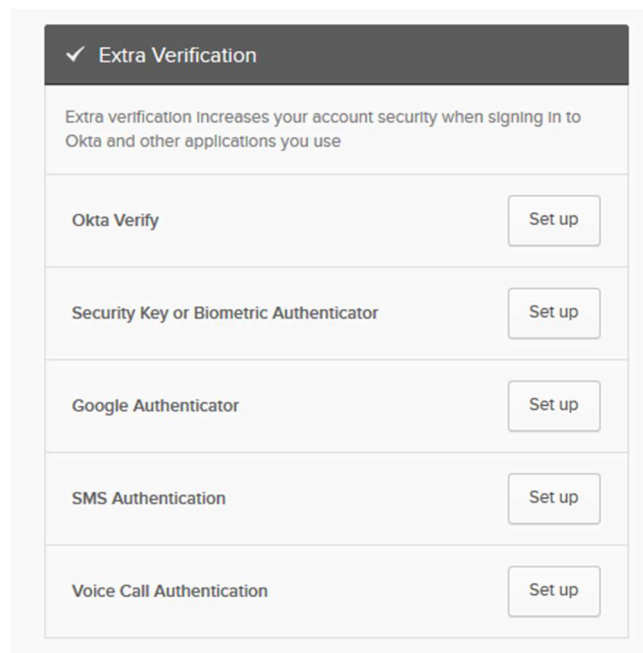
# Setting Up Multifactor Authentication for Okta

**It is recommended to setup more than one authentication factor. If you only have one factor setup and you lose it, you will need to contact support to get your MFA reset.**

Sign in to Okta at <https://e1b.okta.com>, click on your name in the upper right corner, and select Settings



Scroll down the page until you see Extra Verification



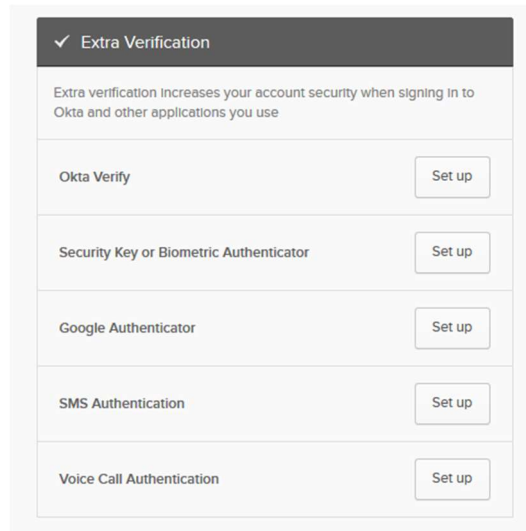
Your options are:

- Okta Verify
- Security Key or Biometric Authenticator
- Google Authenticator
- SMS Authentication
- Voice Call Authentication

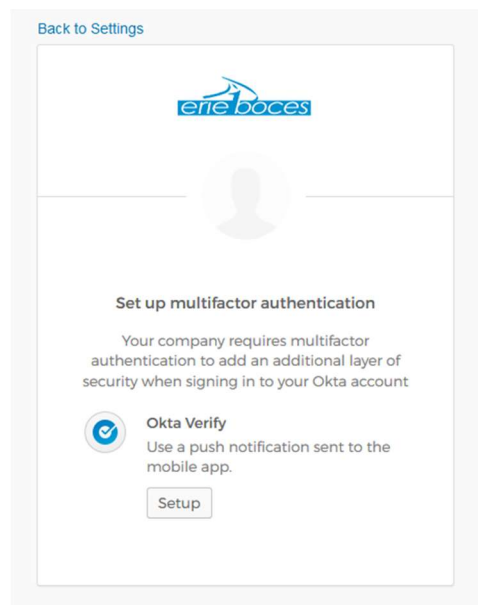
# Okta Verify

Okta Verify is a free mobile app that is installed on a smartphone. It can be found in the Apple AppStore and Google Play Store.

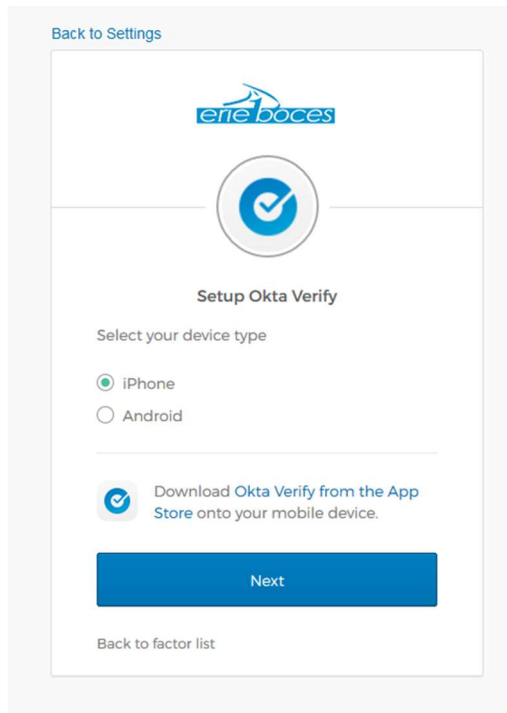
Once installed, go to the settings page following the directions from the first page of this guide. Click on “Set up” next to “Okta Verify”



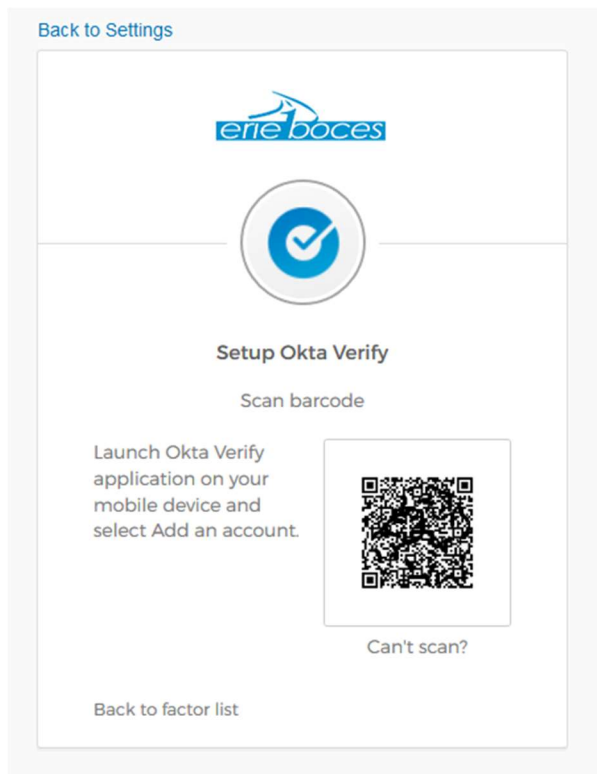
You should now see the “Set up multifactor authentication” screen. Click on “Setup”



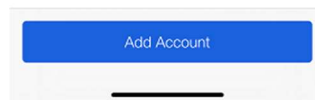
Select which type of smartphone you have and click "Next"



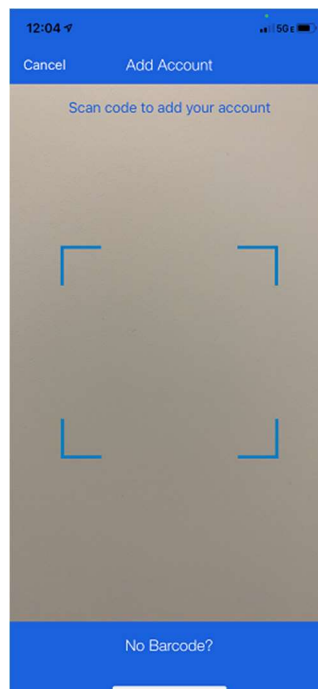
You should see a screen with a barcode on it



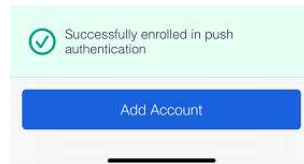
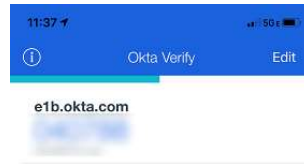
Open the Okta Verify app on your smartphone. Click the “Add Account” button at the bottom of the screen



The app might ask permission to access your camera, if so, allow the app to access it. You should now see a blue box on your smartphone screen. Point your phone's camera to your computer screen and line up the blue box with the barcode on your computer screen

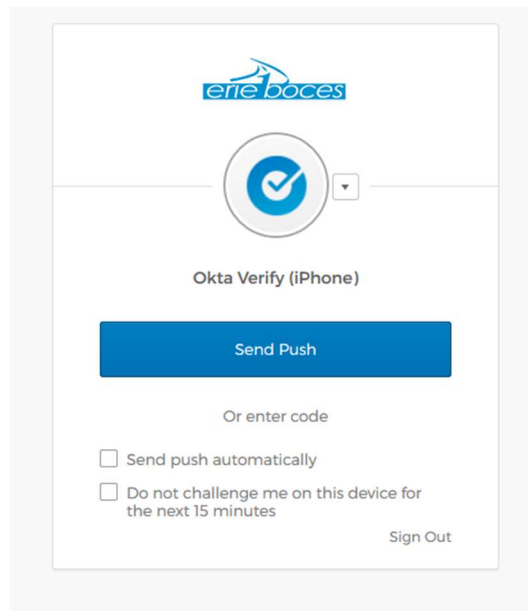


After successfully scanning the barcode you will see “Successfully enrolled in push notification” and should also your email address and a six-digit code listed under “e1b.okta.com”

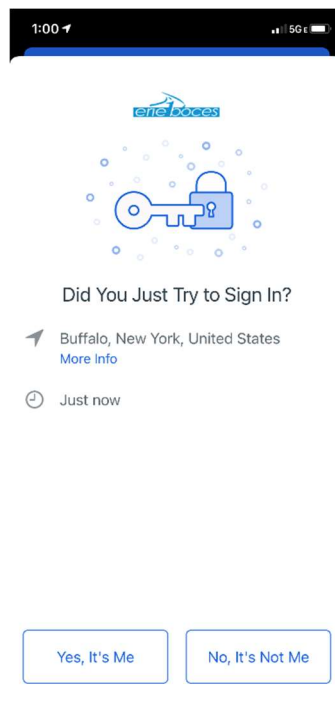


# Signing in with Okta Verify

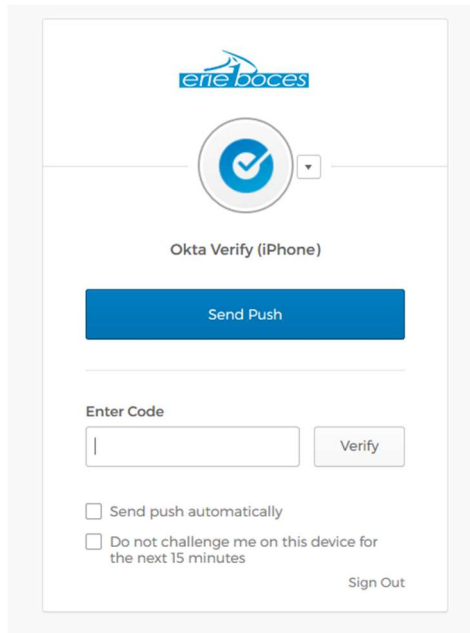
After setting up Okta Verify, at your next login you will be prompted for Multifactor Authentication



Click “Send Push” and you will receive a notification on your smartphone from Okta Verify to confirm your login. You can check the box next to “Send push automatically” and it will automatically send the push notification to your phone at your next login.



If you are in an area where you have no data connectivity on your smartphone, push notifications will not work. To verify your account when signing in, click “Or enter code” and a text box will appear for you to enter a code

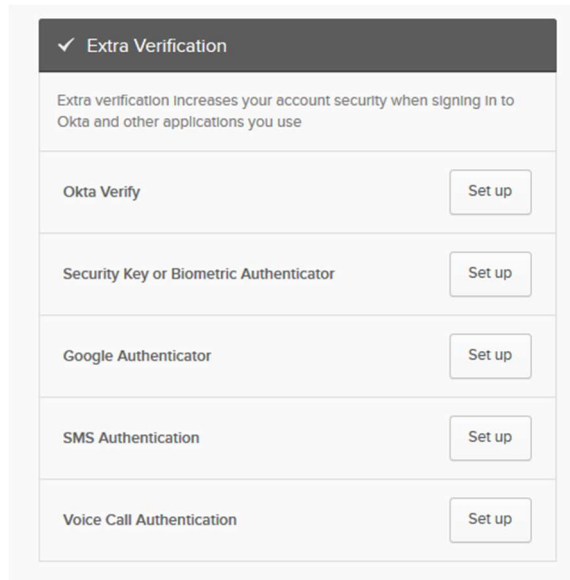


Open the Okta Verify app on your smartphone. You will see “e1b.okta.com” along with a six-digit code and your email address. Enter that six-digit code in the text box and click “Verify”

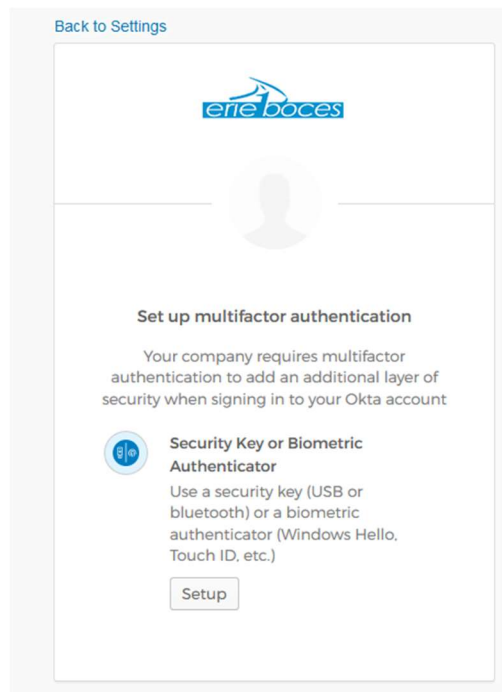


# Security Key or Biometric Authenticator

A security key is a USB device with a button on it. To setup a new security key, go to the settings page following the directions from the first page of this guide. Click on “Set up” next to “Security Key or Biometric Authenticator”

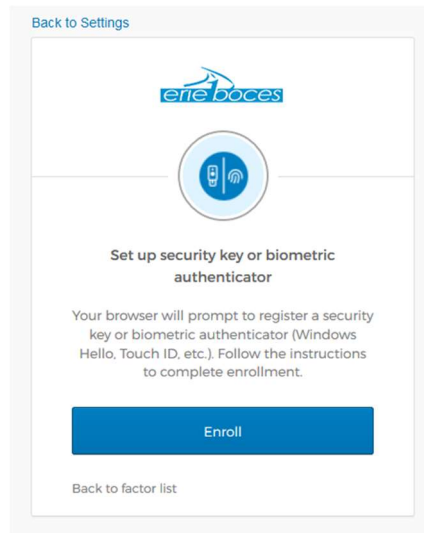


You'll be brought to the “Setup multifactor authentication” page. Click “Setup” under “Security Key or Biometric Authenticator”

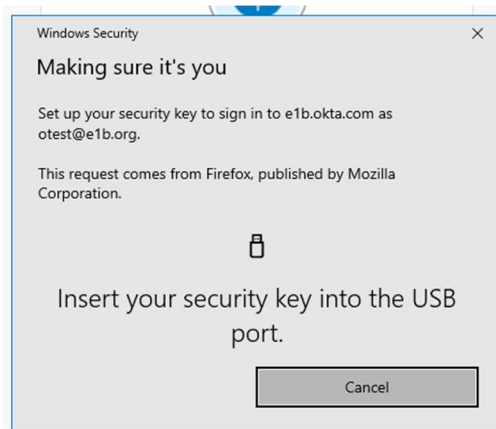




Click the “Enroll” button



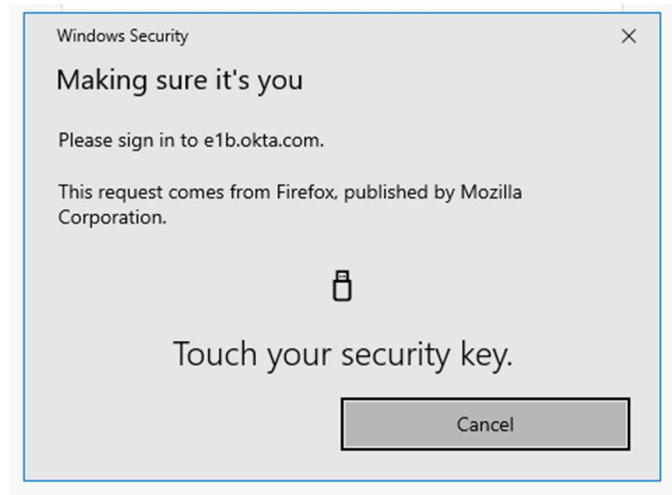
If you haven't already inserted your security key, a prompt will come up for you to insert the key



After inserting the key, the prompt will change and ask you to press the button on the key, and you have completed the security key setup



# Signing in with Security Key

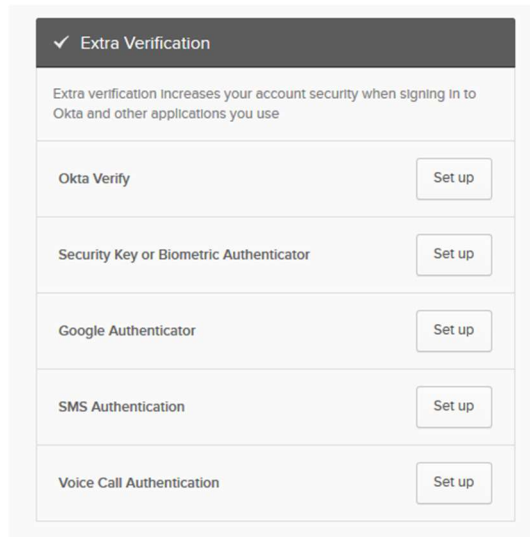


Insert your security key, then press the button on the key. You are now authenticated and redirected to the Okta dashboard

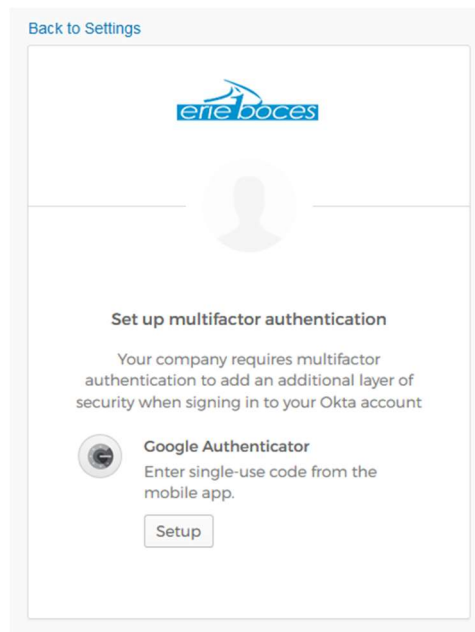
# Google Authenticator

Google Authenticator is a smartphone app that generates 2-Step Verification codes. This will work with other authenticator apps like Authy and Microsoft Authenticator. We'll be using Google Authenticator for this guide.

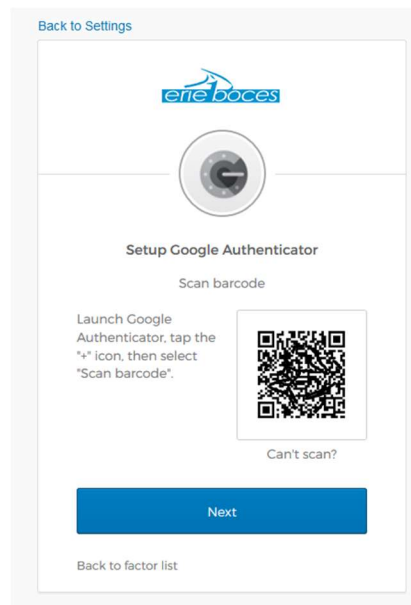
Authenticator apps can be found in the Apple AppStore and Google Play Store. After installing an authenticator app, go to the settings page following the directions from the first page of this guide. Click on "Set up" next to "Google Authenticator"



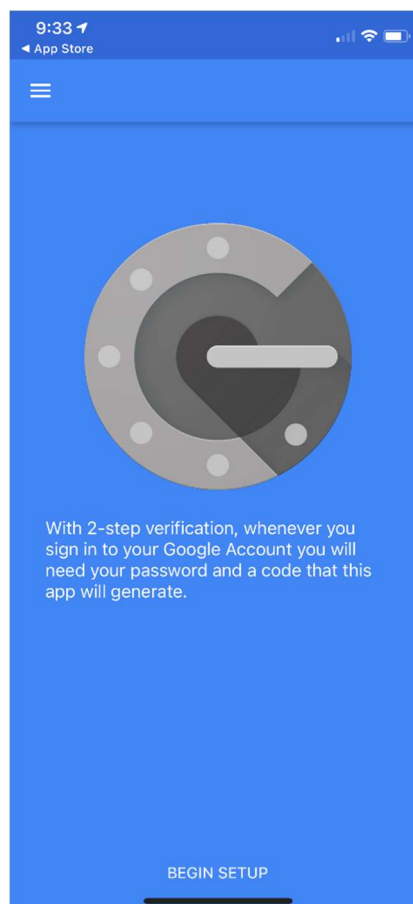
You'll be brought to the "Setup multifactor authentication" page. Click "Setup" under "Google Authenticator"



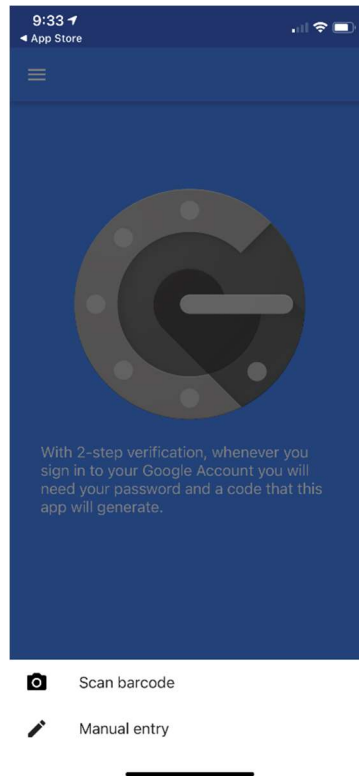
At the Setup Google Authenticator screen, you will be given a QR code to scan



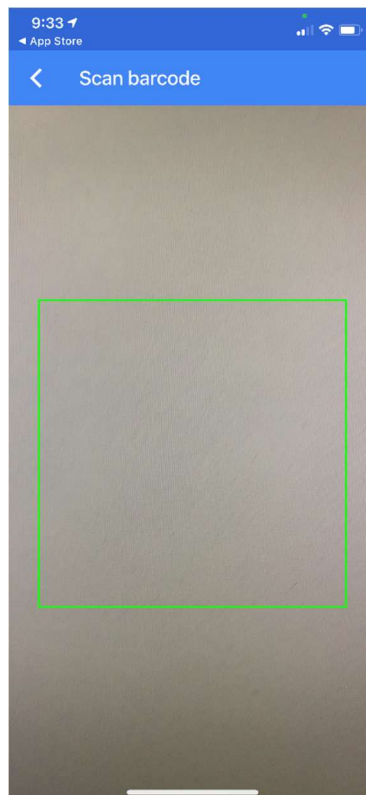
Open the Google Authenticator app on your smartphone and press “Begin Setup”



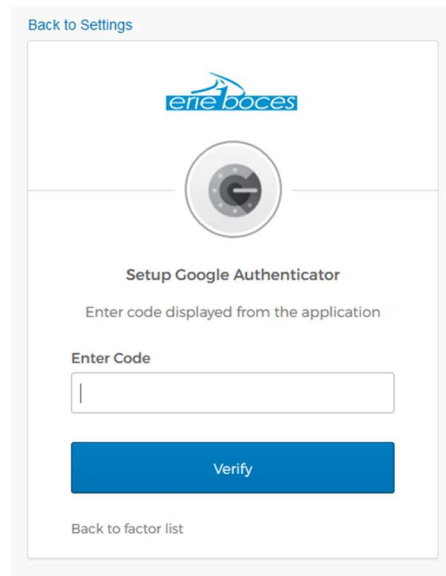
Press "Scan barcode"



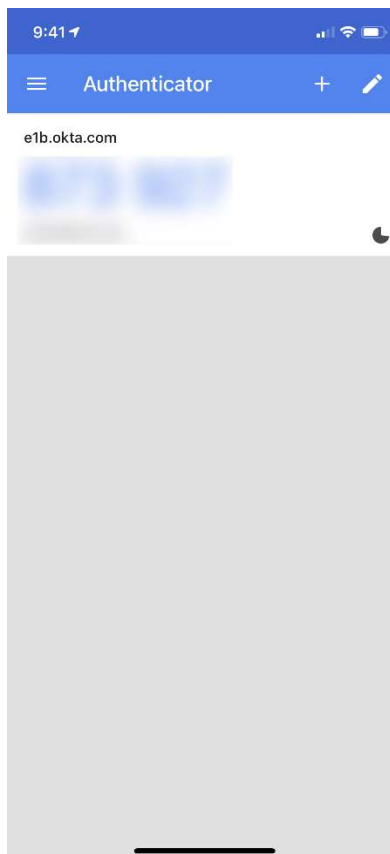
Point your camera at your computer screen and line up the QR code so it's in the green box



After successfully scanning the barcode you will see your email address and a six-digit code listed under “e1b.okta.com.” Click “Next” on the “Setup Google Authenticator” screen on your computer. You’ll be asked to provide a six-digit code. You will find this code in the Google Authenticator app

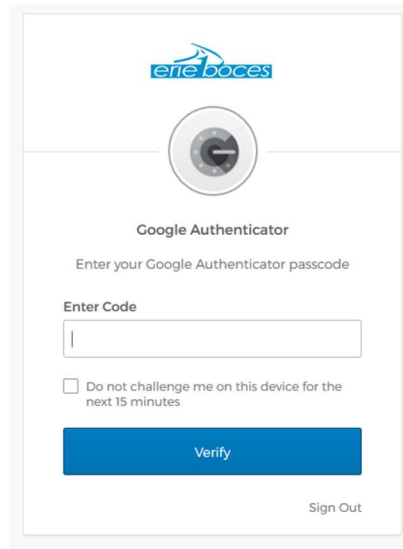


Enter the current six-digit code that you see in the Google Authenticator app and click “Verify”



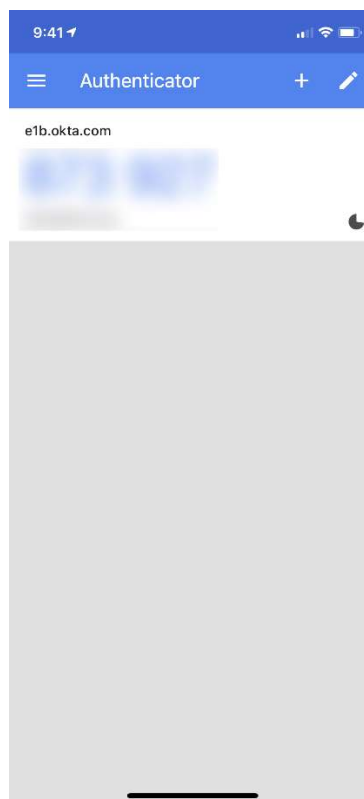
# Signing in with Google Authenticator

After setting up a Google Authenticator, at your next login you will be prompted for Multifactor Authentication



The screenshot shows a web-based login interface for ERIE BOCES. At the top is the ERIE BOCES logo. Below it is a circular icon representing a smartphone. The text reads "Google Authenticator" and "Enter your Google Authenticator passcode". There is a text input field labeled "Enter Code" with a cursor. Below the input field is a checkbox labeled "Do not challenge me on this device for the next 15 minutes". At the bottom, there is a blue "Verify" button and a "Sign Out" link.

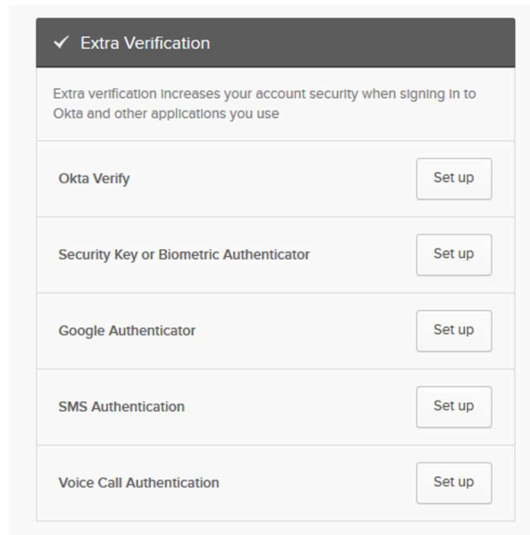
Open Google Authenticator on your smartphone, enter the six-digit code shown in the app into the "Enter Code" box on the sign on screen and click "Verify"



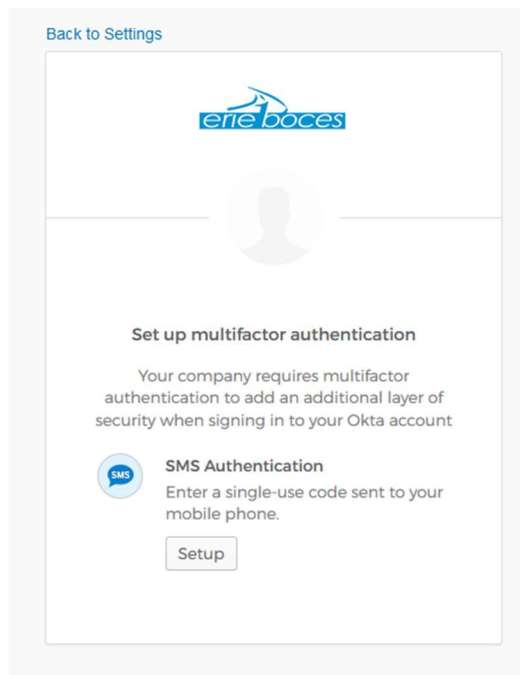
# SMS Authentication

SMS Authentication uses a text message sent to your cell phone. If you do not have an unlimited texting plan, every time you use SMS Authentication a text message will be sent to your phone that will count against your monthly text message allotment.

To setup SMS Authentication, go to the settings page following the directions from the first page of this guide. Click on “Set up” next to “SMS Authentication”



At the “Setup multifactor authentication” screen, click “Setup” under “SMS Authentication”





Enter your cell phone number, area code first, in the “Phone number” box and click “Send Code”

Back to Settings

erie boces

SMS

Receive a code via SMS to authenticate

United States

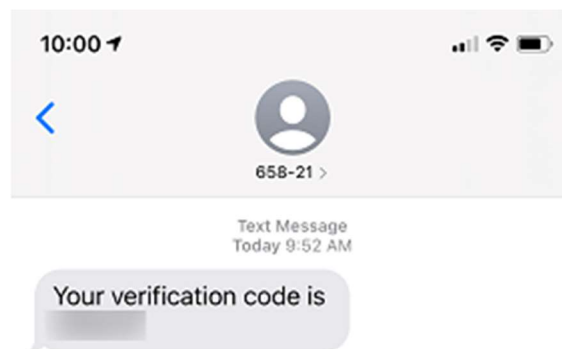
Phone number

+1

Send code

Back to factor list

You should receive a text message on your cell phone



Enter the six-digit code from the text message into the “Enter Code” box and click “Verify”

Back to Settings

erie boces

SMS

Receive a code via SMS to authenticate

United States

Phone number

+1 7163108565 Sent

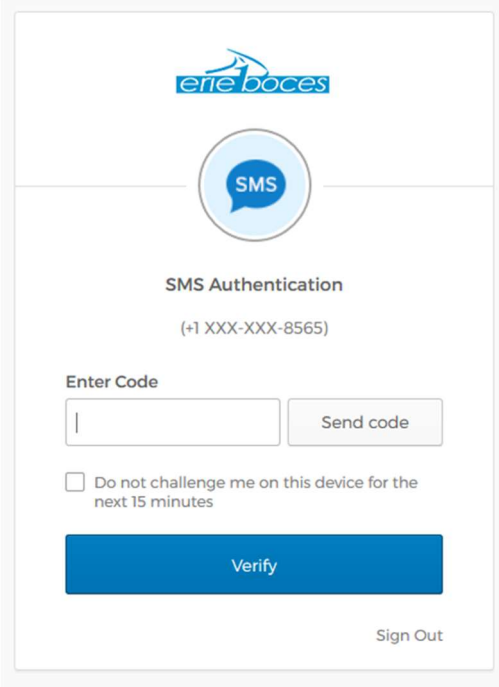
Enter Code

Verify

Back to factor list

# Signing in with SMS Authentication

After setting up a SMS Authentication, at your next login you will be prompted for Multifactor Authentication



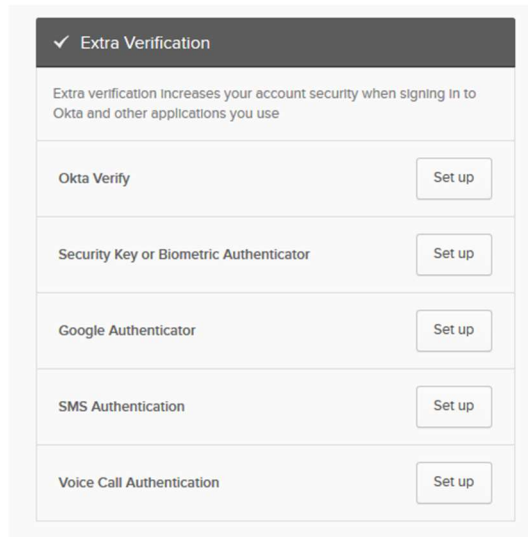
The screenshot shows a login interface for Erie 1 BOCES. At the top is the Erie 1 BOCES logo. Below it is a circular icon with 'SMS' inside. The text 'SMS Authentication' and the phone number '(+1 XXX-XXX-8565)' are displayed. There is an 'Enter Code' label above a text input field. To the right of the input field is a 'Send code' button. Below the input field is a checkbox with the text 'Do not challenge me on this device for the next 15 minutes'. At the bottom is a large blue 'Verify' button and a 'Sign Out' link.

Click “Send code” and a text message will be sent to your phone. Enter the six-digit code from the text message and click “Verify”

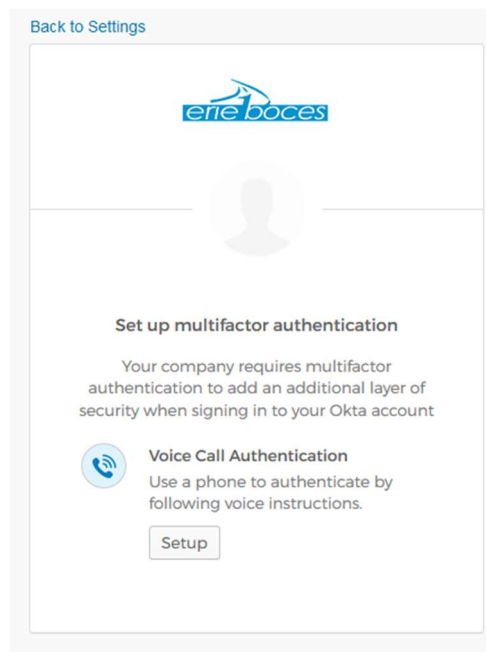
# Voice Call Authentication

Voice Call Authentication uses an automated calling system to call you and give you a five-digit code. This works with cell, VoIP, and landline phones. If you do not have an unlimited phone plan, this call will count against your monthly allotted minutes.

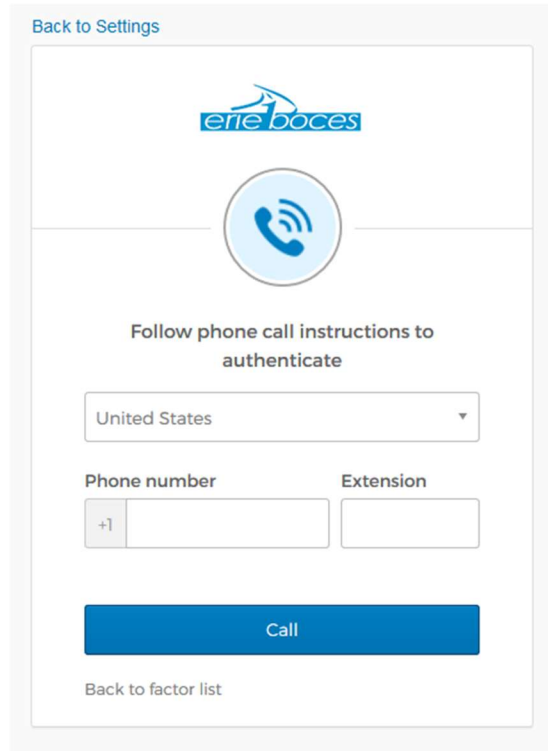
To setup Voice Call Authentication, go to the settings page following the directions from the first page of this guide. Click on “Set up” next to “Voice Call Authentication”




At the “Set up multifactor authentication” screen, click on “Setup” under “Voice Call Authentication”




Enter the phone number you would like to receive the call at in the “Phone number” box. If an extension needs to be used, enter that in the “Extension” box. Click the “Call” button



Back to Settings





Follow phone call instructions to authenticate

United States

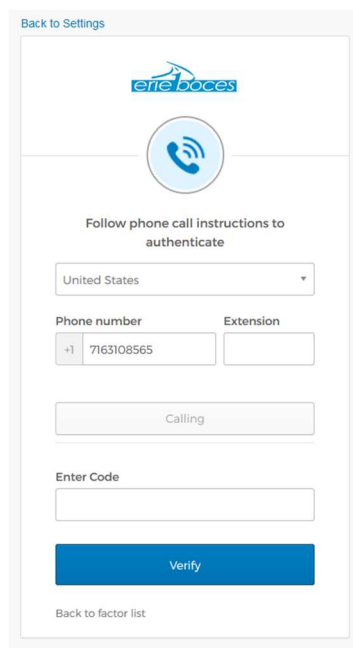
Phone number      Extension

+1


**Call**


Back to factor list

You will receive an automated call at the number you entered. An automated voice will read a five-digit code twice, then hang up. Enter that five-digit code into the “Enter Code” box and click “Verify”



Back to Settings





Follow phone call instructions to authenticate

United States

Phone number      Extension

+1 7163108565

Calling

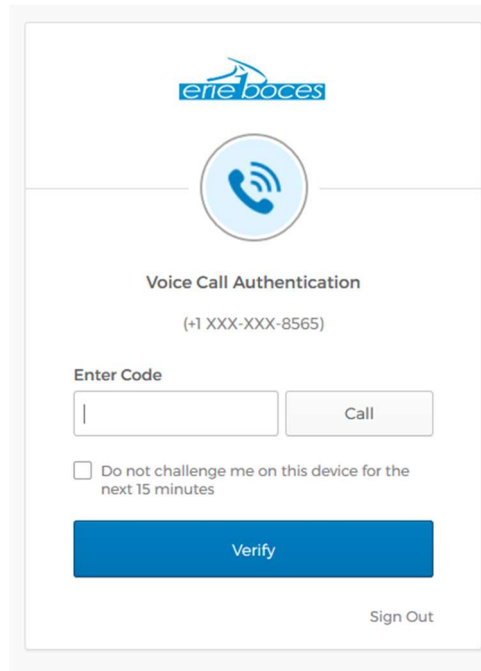
Enter Code

**Verify**

Back to factor list

# Signing in with Voice Call Authentication

After setting up a Voice Call Authentication, at your next login you will be prompted for Multifactor Authentication



The screenshot shows a login interface for Erie BOCES. At the top is the Erie BOCES logo. Below it is a circular icon with a telephone handset and signal waves. The text reads "Voice Call Authentication" followed by the phone number "(+1 XXX-XXX-8565)". There is an "Enter Code" label above a text input field and a "Call" button. Below the input field is a checkbox labeled "Do not challenge me on this device for the next 15 minutes". At the bottom is a large blue "Verify" button and a "Sign Out" link.

Click the "Call" button. You will receive a call and have a five-digit number read to you. Enter the number in the "Enter Code" box and click "Verify"